UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/769,104	01/30/2004	Catalin D. Sandu	MSFT122167	9006

26389 7590 05/02/2007

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
HAILU, TESHOME	
ART UNIT	**PAPER NUMBER**
2109	
MAIL DATE	**DELIVERY MODE**
05/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/769,104	SANDU ET AL.	
	Examiner	Art Unit	
	Teshome Hailu	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01/30/04*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01/30/04* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5 are pending.

Specification

2. The disclosure is objected to because of the following informalities: The "**normalization module 204**" on page 7 line 20, 23 and 25 should be "normalization module 202". Appropriate correction is required.

3. The disclosure is objected to because of the following informalities: On page 9 line 13, the use of the trademark **"Visual Basic"** has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology. Appropriate correction is required.

4. The disclosure is objected to because of the following informalities: On page 12 line 19, the use of the trademark **"Microsoft Corporation's Visual Basic Script"** has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology. Appropriate correction is required.

5. The disclosure is objected to because of the following informalities: On page 13 line 25-26, the use of the trademark **"Visual Basic script or JavaScript"** has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology. Appropriate correction is required.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-5 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-5 are directed to functional descriptive material, which consists of a computer program per se that detect if the executable script is a malware. Since a computer program by itself, (i.e., without computer readable and/or storable medium), is not a process and does not fall within the statutory classes listed in 35 U.S.C. 101. The claims are believed to recite non-statuary subject matter. The examiner has suggested that a computer hardware implementation needs to be added to the invention.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-5 are rejected under 35 U.S.C. 102(e) as being anticipated by Ho et al (Ho), US 7,188,369.

As per claim 1, Ho discloses:

- A malware detection system (column 1, line 50-51, "The invention generally provides an **antivirus network system**"). According to the invention, "***a malware is defined as unwanted computer attacks***", which implies that an antivirus is one kind of malware detection system.

- for determining whether an executable script is malware according to its functionality (column 2, line 13-16, "**The antivirus virtual scanning processor** advantageously allows quick and efficiently dispatched patches in performing and delivering **antivirus functionalities** for newly discovered **computer viruses**.")

- a malware signature store including at least one known malware script signature (Abstract, line 6, "**an antivirus database** comprising a **plurality of computer virus signatures**"), where the **antivirus database** further explained as (column4, line 9-10, "**storing** a plurality of computer **virus signature**").

- a normalization module that obtains an executable script, and normalizes an executable script, thereby generating a script signature for the executable script. (Column 4, line 38-42, "The processor emulator 102 is operable to execute the internal instruction 1, 2, 3, ... M in detecting computer viruses by, e.g., **scanning data in the system in comparison with the plurality of virus signatures in the signature database201**"). Detecting computer viruses by scanning data in comparison with stored

virus signatures inherently indicates that the pattern (signature) of the data is obtained (created) and compared against stored signature.

- detection system compares the script signature for the executable script **to the at least one script** ***signature in the malware signature store*** *(column 4, line 33-35,* "The scanning module 100 **compares data files** in a computer or network system **with the patterns inside a virus pattern file**"), where a virus pattern file is further explained as (column 4, line 31-33, "**a database of the binary patterns of a known computer viruses**").

- to determine whether the executable script is malware (column 2, line 64-66, "The scanning module 100 is a program that does actual work of scanning files in a computer or network system and **detecting computer viruses therein, if any**.")

As per claim 2, the rejection of claim 1 is incorporated and further Ho discloses:

- The malware detection system comprising a comparison module, and wherein the comparison module compares the script signature for executable script to at least one script signature in the malware signature store *(column 4, line 33-35,* "The scanning module 100 **compares data files** in a computer or network system **with the patterns inside a virus pattern file**"), where virus a pattern file is further explained as (column 4, line 31-33, "**a database of the binary patterns of a known computer viruses**").

- for the malware detection system (column 2, line 66, "**detecting computer viruses** therein, if any.")

Claim 3 is rejected under the same reason set forth in rejection of claim 1 and further Ho teaches:

- a malware signature storage means (column 4, line 9-10, "a computer virus signature database 201 **storing a plurality of computer virus signatures**"),

- normalization means (column 4, line 38-41, "**scanning data in the system in comparison** with the plurality of virus signatures in the signature database201"). According to the invention, normalization means translating the functional contents of the executable script into a common, "normal" format referred to as a script signature. Ho teaches, by scanning data in comparison with stored virus signatures inherently indicates that the signature of the data is created.

- a comparison means that compares the script signature for the executable script to the at least one script signature in the malware signature storage means (column 6, line 16-19, "in detection computer viruses by, e.g, scanning data in the system in **comparison with the plurality of virus signatures in the signature database** 201".)

Claim 4 is rejected under the same reason set forth in rejection of claim 1 and further Ho teaches:

- A method for determining whether a computer-executable script is a malware script (abstract, line 10-13, "a virtual scanning processor further comprising a

processor emulator operable to execute a plurality of internal antivirus instruction in **detection computer viruses** based on the virus signatures").

- Obtaining an executable script: (column 4, line 38-39, "The processor emulator 102 is operable to **execute the internal instruction** 1, 2, 3, . . ., M in detection computer viruses.")

Claim 5 is rejected under the same reason set forth in rejection of claims 1, 3, 4 and further Ho teaches:

- A computer-readable medium bearing computer-executable instructions (column 3, line 32-35, "A preferred embodiment of the antivirus method for a **computer or network system** according to the invention primarily comprises the steps of operating an antivirus scanning module with an operating system (OS)"). Computer or network system can be conceded as computer-readable medium.

Conclusion

9. The prior art made or record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: Network anti-virus system, US 7152164.

TITLE: Computer immune system and method for detection unwanted code in a computer system, US 7093239.

TITLE: Virus scanning on thin client devices using programmable assembly language, US 6792543.

TITLE: Computer security using virus probing US 6205551.

TITLE: Data mining method for detection of new malicious executables, Authors: Schultz et al. 14-16 May 2001, IEEE.

TITLE: Computer security: Neutralizing windows-bases malicious mobile code, Authors: James et al. March 2002, ACM.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Teshome Hailu whose telephone number is (571) 270-3159. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m. PST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chamili Das can be reached on (571) 272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Chamili Das

CHAMELI DAS
SUPERVISORY PATENT EXAMINER

4/24/07.

TH